

REMARKS/ARGUMENTS

Applicants thank the Examiner for her courtesy and consideration in discussing this Application in a telephone interview on October 17, 2006. Because interviews after final are discretionary, Applicants especially appreciate the opportunity.

The claims were discussed in light of the cited references, and certain possible amendments were addressed. Although there was no specific agreement, an understanding was reached regarding certain claim interpretations and potential areas of novelty. The claims, as amended herein, are drafted to reflect the discussion with the Examiner regarding possible claim amendments. For certain claims, additional specificity is included regarding the functions performed by the smart card and central computer system, to address concerns raised by the Examiner.

Status of the Claims

Before this Amendment, claims 1, 2, 4-18, 20-27, 29-35 and 59 were examined. Claims 1, 17, 18, 21, 22, and 29 are amended to more particularly claim certain embodiments of the invention, and support for the amendments may be found in the Specification (Original Application, p. 9. ll. 18-20, 34). No claims are presently added or canceled. Therefore, claims 1, 2, 4-18, 20-27, 29-35, and 59 remain present for examination, and claims 1, 17, 18, 21, 22, 25, and 29 are the independent claims. Reconsideration is respectfully requested, and a Request for Continued Examination is submitted concurrently herewith..

The Final Office Action dated August 10, 2006 ("Final Office Action") rejected claims 1, 2, 4-17, 29-35 under 35 U.S.C. §103(a) as unpatentable over the cited portions of U.S. Patent 6,101,477 to Hohle et al. ("Hohle") in view of the cited portions of U.S. Patent 5,745,571 to Zuk ("Zuk") and further in view of the cited portions of U.S. Patent 6,304,223 to Hilton et al. ("Hilton"). The Final Office Action rejected claims 18, 20, and 22-27 under 35 U.S.C. §103(a) as unpatentable over the cited portions of U.S. Patent 6,226,744 to Murphy et al. ("Murphy") in view of Hilton and Zuk. The Final Office Action rejected claim 21 under 35 U.S.C. §103(a) as being unpatentable over Hohle in view of Murphy and Hilton.

35 U.S.C. §103(a) Rejections, Hohle et al.

The Final Office Action rejected independent claims 1, 17, 21, and 29 under 35 U.S.C. §103(a) as unpatentable over Hohle and various combinations of references cited above. Various embodiments of the present invention comprise systems or methods for establishing a secure communication link *between a smart card and a central computer system*. To establish a *prima facie* case of obviousness, the prior art references must "teach or suggest all the claim limitations." MPEP §2143.

The cited references cannot be relied upon to teach or suggest the limitations of independent claims. Specifically, the references fail to teach 1) secured data formatted to allow the central computer system to detect a modification to the secured data occurring during transmission beginning at the smart card and extending through to the central computer system, as recited in claims 1, 17, 21, 22 or 29, or 2) a second set of secured data, the second set formatted to allow the smart card to detect a modification to the second set occurring during transmission beginning at the central computer system and extending to the smart card, as recited in claim 17, 18, 25.

Claims 1, 17, 21, 22 and 29 describe the secure data exchanged between the smart card and the central computer system. The secure data is formatted by the smart card to allow the central computer system to detect a modification to the secured data occurring during transmission, beginning at the smart card and extending through to the central computer system. This particular form of end-to-end data integrity is not taught or suggested by the references. The end-to-end processing, from smart card to the central computer system, provides a mechanism to ensure that a packet has not been modified at any point between the smart card and the central computer system. This end-to-end processing allows the smart card to send a packet to the central computer system to process a transaction without requiring intermediate network elements to further interpret the *content* of that packet. Thus, in certain embodiments the contents of the packet need "not [be] deciphered, decoded or authenticated anywhere within the communication link except at the smart card 106 and the smart card server 130" located in the central computer system 102 (Original Application, p. 10, ll. 7-9).

Independent claims 17, 18 and 25 further set forth embodiments wherein, for transmission in the opposite direction, a smart card may detect a modification to the secured data beginning at the central computer and extending through to the smart card.

The Final Office Action relies on Hohle to teach these limitations (Final Office Action, p. 2; p. 4, ll. 5-6; p. 8, l. 3; p. 10, ll. 15-16, *citing* Hohle, col. 22, ll. 47-67). But the cited portions of Hohle fall far short of teaching the identified limitations, instead teaching "'signing' of the data using a message authentication code" for transmission between the "card" and "external device" (Hohle, p. 22, ll. 50-57). This "signing," however, falls far short of the end-to-end connectivity of the claims. The use of the MAC in Hohle is to authenticate content only between the card and an "external device." This clearly differs from the claims, which describe end-to-end data integrity between the smart card and the central computer system. The central computer system in certain embodiments is configured to process a transaction for the smart card using the data formatted by the smart card.

The Office Action indicates that it is the issuer 10 of Hohle that reads on the central computer system of the claims (Final Office Action, p. 3, *citing* Hohle Fig. 10). But there is simply no suggestion that the use of the message authentication code for "signing" data be from the smart card to that issuer 10. There is no teaching or suggestion that the "external device" of Hohle comprises the issuer 10. The use of a message authentication code between a card and an intermediate device, as suggested by Hohle, clearly falls short of the end-to-end data integrity of the claims.

The Final Office Action further relies on Hohle to teach certain encryption and authentication for a smartcard system. While Hohle may describe user "authentication" and data "encryption," there is no teaching or suggestion of the claimed end-to end form of data integrity beginning at the smart card and extending through to the central computer system. Hohle fails to describe the functionality of the system to "detect a modification to the secured data" throughout the transmission in the manner set forth in the claimed embodiments.

Implicitly, the Office admits that Murphy, Hilton, and Zuk fall short of teaching this limitation as well. Because it is asserted that the cited references do not teach the limitations at issue, it is respectfully submitted that independent claims 1, 17, 18, 21, 22, 25, and 29 are allowable. Claims 2, 4-16, 20, 23, 24, 26, 27, 30-35, and 59 each depend from the independent claims, and these claims are believed allowable for at least the same reasons as given above. Applicants, therefore, respectfully request that the rejections under 35 U.S.C. 103(a) be withdrawn.

Respectfully submitted,



Michael L. Drapkin
Reg. No. 55,127

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
MLD:klb
60904600 v1